

SN3262 – Network Administration, Management and Security

Exercise 1: Using Linux Commands to Investigate a Sub-network

Brief Outline Answers

Since we will be wanting to look at some simple command line ‘programs’ written in the form of scripts you must be familiar with the material in Exercise 0 and with the various ‘network utilities’ such as *ifconfig*, *netstat*, *ping* and *traceroute*.

1. By reading through the man pages of *ifconfig* what would you say is the function of *ifconfig*?
To configure the kernel-resident network interfaces and display the status of the currently active interfaces.
2. How, previously, have you used *ifconfig*?
Probably Only to display the status of the network interface card.
3. What would you have to be/have to use this command with the various options?
Root or have super user rights.
4. By reading through the man pages of *ping* what would you say is the function of *ping*?
To provide information of host connectivity and round trip times.
5. If you use broadcast *ping* with the *-c 1* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, how many responses would you get and why?
One — from the sending node. As soon as a reply is received ping stops.
6. If you use broadcast *ping* with the *-c 2* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, how many responses would you get and why?
Eleven — one response from each node to the first echo request and only one response from the sending node to the second echo request.
7. In the latter case how many of the responses would be marked as duplicates and why?
Nine — these are responses to the first of the echo requests from nodes other than the sending node.
8. What is the default interval between ‘pings’ and how can it be altered?
One second. It can be altered with the *-i* option.
9. What would the command *ping 149.170.11.33 -f 0* do and why would you not be able to successfully execute this command?
Flood ping (i.e. send pings as fast as possible) the node 149.170.11.33. Only super-user can use this option.
10. What does the command *ping 149.170.11.33 -l 3* do?
Pre-loads 3 packets that are sent without waiting for a reply.
11. What does the command *ping 149.170.11.33 -i 0.1* do and why would you not be able to successfully execute this command?
Sets the interval between pings to the node 149.170.11.33 to 0.1 s. Only super-user can set intervals less than 0.2 seconds.

12. What might the command *ping www.mmu.ac.uk -R* do?

Display the route buffer on returned packets.

13. If you use broadcast *ping* with the *-w 1* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, how many responses would you get and why?

Ten. Receive times-out after 1 second.

14. How would the responses to a broadcast *ping* with the *-c 2* option on a local subnet to which 10 devices, including the broadcasting device, (all set up to respond to broadcast) are attached, differ from the responses with the *-w 1* option?

With the *-c 2* option there are 11 responses — see question 6, with the *-w 1* option there are 10 — see question 13.

15. By reading through the man pages of *traceroute* what would you say is the function of *traceroute*?

Track the route that packets follow to some host.

16. *traceroute* normally uses UDP packets. What mechanism is used to “prevent” the receiving host from processing the UDP packet?

The destination port is set to an unlikely value.

17. When *traceroute* is used on a local subnet with the IP address of a host on the subnet which is ‘up’ what information does *traceroute* return?

Number of hops to target, the name (if available) of the target and three round trip times.

18. If *traceroute* is used on a local subnet with the IP address of a host on the subnet which is ‘down’ how are the round trip times printed and what does it mean?

!H is printed after a default timeout (about 3 seconds).

19. When *traceroute* is used for a host that is several ‘hops’ away and a router along the path does not send ICMP “time exceeded” messages how is this shown in the output from *traceroute*?

Three “*”s.

21. Use *gawk* to print out the first two fields of the line in the /etc/hosts file that contains the IP address 149.170.13.8. Write down the command line that you used and the output that you obtained.

**gawk '/149.170.13.8/ {print \$1, \$2}' /etc/hosts
149.170.13.8 hardy.doc.stu.mmu.ac.uk**

22. Create a file as follows:

150.100.100.10: bill
150.100.100.11: fred
150.100.100.12: jim

Use *cat* to list the file and pipe it through *sed* to remove the colons and redirect the output to another file. Check the contents of the file and write down the command line that you used.

cat names | sed 's/:/ /'

23. Read the man pages for *ps*. By piping the output of *ps -ef* to *gawk* determine the number of processes that are running under your user id at the time of running the command — exclude the process for *ps -ef*. *A possible solution:*

ps -ef | gawk '{if((\$1 == "johnh") && (\$8 != "ps")) ++tot} END {print tot}'